ABSTRACT OF THE DISCLOSURE

An Internet appliance has added hardware and software functionality to allow communication where a dialing action request is authorization is verified using a personal identification means (PIM). A user first selects a communication access number by requesting a dialing action on a actual or a virtual keypad or by clicking a "hot spot" on a Web page. Selecting an access number (e.g., dialing of a telephone number), alerts the user of the Internet appliance of the selection process whether the user instigates or the selection is attempted from a remote device using the Internet appliance facilities. Either method will trigger software commands that prompt the user to enter a PIM either to authorize his own use or another one's use of the Internet appliance. The PIM may comprise, but is not limited to, keying in a personal identification number (PIN), a biometric identification, or a smart card stored number. The PIM is correlated to an authorization means that verifies that the user so identified is authorized to make or allow the prescribed connection. The Internet appliance has a security protocol that is used to encrypt and decrypt the PIM data. Also the device drivers used to execute a dialing action are also encrypted by the security protocol and are only decrypted on granting of authorized use of the Internet appliance. If the user so requests and is authorized, they may also select to use the security protocol to execute secure communication. The security protocol includes but is not limited to a Public/Private symmetric key technology.